From: Golden, Valerie (HSC)
To:

Subject: Do you have a Contingency Plan?
Date: Friday, May 12, 2017 3:01:56 PM

Good afternoon, Health Care Components – This is a good reminder of the importance to develop a contingency plan for responding to emergencies or other events that may damage systems that contain ePHI. If you haven't already done so, please send me your Disaster Recovery plan for systems that process and/or store ePHI.

Hospitals in UK National Health Service knocked offline by massive ransomware attack

The National Health Service in England and Scotland was hit by a large ransomware attack that has affected at least 16 of its organizations, NHS Digital announced this morning.

The attackers are asking for 415,000 pounds, or about $534,146, before May 19 or the hackers will delete the files.

The attack has crippled the health system's ability to treat patients, according to BBC News. Hospital staff are unable to access patient data. Further, ambulances are being diverted and patients are being warned to avoid some departments.

The organization launched an investigation and determined the ransomware is likely the Wanna Decrytor. It's one of the most effective ransomware variants on the dark web, and at the moment, there is no decryptor available.

Officials said the attack didn't specifically target the agency and that organizations from other sectors have been hit, as well.

"At this stage we do not have any evidence that patient data has been accessed," officials said in a statement.

NHS Digital is working closely with National Cyber Security Centre, the Department of Health and NHS England to help the organizations affected by the attack and to ensure patients are protected.

"Our focus is on supporting organizations to manage the incident swiftly and decisively, officials said. "But we will continue to communicate with NHS colleagues and will share more information as it becomes available."

Valerie Golden
HIPAA Security Officer
(405)271-8001 x46456

CONFIDENTIALITY NOTICE: This email, which includes any files transmitted with it, contains confidential information from University Legal Counsel, is intended solely for the use of the individual or entity to whom it is addressed, and may contain information protected by the attorney-client privilege. If you are not the intended recipient or the person responsible for delivering this email to the intended recipient, be advised that any use, dissemination, forwarding, printing, or copying of this email is strictly prohibited. If you have received this email in error, please notify the sender immediately by a "reply to sender only" message and destroy all electronic and hard copies of this email and any attached files.

From: Golden, Valerie (HSC)
Sent: Tuesday, February 7, 2017 2:56 PM
Subject: Documented Downtime Procedure/Plan for Systems that Process or Store ePHI

Good afternoon, Health Care Components

The University's Contingency Plans for ePHI Policy (HIPAA Security #07, effective 1-2-14, http://www.ouhsc.edu/Portals/0/Assets/Documents/hipaa-security/SEC07%20-%20Contingency%20policy-clean%2010_24_16.pdf) requires that each Health Care Component document its preparedness for emergencies or disasters such that electronic Protected Health Information is protected and available and the HCC is able to continue providing services, as appropriate.

While this policy appears to be directed at Information Technology, each HCC is responsible for documenting a Disaster Recovery plan for systems that process and/or store ePHI. The plan should be available to all workforce members and should include at a minimum:

1. What actions are to be taken.
2. Responsibilities for workforce members.
3. Key personnel and contact information.
4. Key contractors, subcontractors, vendors, business associates, and contact information.
5. Procedures for ensuring business continuity.
6. Emergency response procedures for workforce members.

The plan should be tested and reviewed annually. In addition, Disaster Recovery training should be performed annually.

My understanding is that many HCCs have general procedures for the above, but they have not documented those procedures, as required by HIPAA. If your area has neither written nor unwritten procedures, I have attached a sample procedure document that you may revise to fit your HCC.

Sample logs for key personnel and contractor/vendor contact information are attached. If your HCC relies on your Tier 1 or IT Representative to address any or all of the above items, there must be an IT Service Level Agreement in place between your HCC and IT that documents those responsibilities.

Please provide your documentation of preparedness to me no later than March 3, 2017. I will send you confirmation that your procedures and forms comply with the current policy and will ask at that time that you send a copy to your staff, letting them know where the hard-copy of the procedures will be located within your clinic or department. This policy will be included in our HIPAA Security audits. If you need assistance with your draft, please contact me and I will assist you or put you in touch with someone who can.

I appreciate your help in making sure your HCC and the University are in compliance with HIPAA. If you have any questions about this email or the attached sample procedures, please let me know.

Valerie Golden, RHIA
HIPAA Security Officer
Office of Compliance
The University of Oklahoma
(405)271-8001 x46456

CONFIDENTIALITY NOTICE: This email, which includes any files transmitted with it, contains confidential information from University Legal Counsel, is intended solely for the use of the individual or entity to whom it is addressed, and may contain information protected by the attorney-client privilege. If you are not the intended recipient or the person responsible for delivering this email to the intended recipient, be advised that any use, dissemination, forwarding, printing, or copying of this email is strictly prohibited. If you have received this email in error, please notify the sender immediately by a "reply to sender only" message and destroy all electronic and hard copies of this email and any attached files.